In the Claims;

Please cancel claim 16 without prejudice or dedication.

Please amend the below claims as indicated.

1. (Currently Amended) A method of providing security against unauthorized access to internal resources of a network device comprising:

receiving a digital signature at a security association manager (SAM); ~~wherein said digital signature includes an encryption code~~;

said SAM requesting a de-encryption code;

said SAM de-encrypting said digital signature with said de-encryption code;

said SAM authenticating said de-encrypted digital signature; ~~and~~

said SAM, responsive to said authenticating of said de-encrypted digital signature, obtaining an access level for program code associated with said digital signature; and

said SAM, responsive to said obtained access level, requesting allowed operations, said allowed operations using said internal resources of said network device, said allowed operations associated with said access level, said requesting responsive to processing of said program code. ~~authenticated signature.~~

2. (Original) A method of providing security according to Claim 1 wherein said network device comprises a Java enabled device.

3. (Currently Amended) A method of providing security according to Claim 1 wherein said ~~encryption code comprises a private key and said~~ de-encryption code comprises a public key certificate ~~associated with said private key~~.

4. (Original) A method of providing security according to Claim 1 further comprising:

a certificate authority receiving said request for a de-encryption code and comparing information in said request to information stored in said certificate authority.

5. (Original) A method of providing security according to Claim 4 further comprising:

said certificate authority responding to said request by sending said de-encryption code to said SAM.

6. (Currently Amended) ~~A method of providing security according to Claim 1 further comprising:~~ A method of providing security against unauthorized access to internal resources of a network device comprising:

receiving a digital signature at a security association manager (SAM);

said SAM requesting a de-encryption code;

said SAM de-encrypting said digital signature with said de-encryption code;

said SAM authenticating said de-encrypted digital signature;

said SAM requesting allowed operations associated with said authenticated signature;

a policy server receiving said request for allowed operations associated with said authenticated signature;

said policy server comparing said authenticated signature with information stored on said policy server; and

said policy server sending a response to said SAM indicating an access level corresponding to said authenticated signature.

7. (Original) A method of providing security according to Claim 6 further comprising:

said policy server authenticating said request for allowed operations associated with said authenticated signature prior to comparing said authenticated signature with said information stored on said policy server.

8. (Currently Amended) Apparatus for providing security against unauthorized access to internal resources of a network device comprising:

a security association manager (SAM)~~;~~ configured to receive a digital signature ~~including an encryption code~~;

wherein said SAM is configured to send a message including a portion of said digital signature;

wherein said message includes a request for an encryption decoder;

wherein said SAM is further configured to receive a response to said message including said encryption decoder; and

wherein said SAM is configured to send a digitally signed message requesting an access level for program code associated with said digital signature, wherein said access level is associated with at least one allowed operation using said internal resources of said network device responsive to processing of said program code ~~allowed operations associated with said digital signature in response to receiving said replay message~~.

9. (Currently Amended) Apparatus for supplying security in accordance with Claim 8 further comprising:

a certificate authority configured to receive said message from said SAM, and to send said response ~~reply.; wherein said certificate authority includes~~

10. (Original) Apparatus for providing security according to Claim 8 wherein said network device comprises a Java enabled device.

11. (Currently Amended) Apparatus for providing security according to Claim 8 wherein ~~said encryption code comprises a private key and~~ said encryption decoder comprises a public key certificate ~~associated with said private key~~.

12. (Currently Amended) ~~Apparatus for providing security according to Claim 8 further comprising:~~ Apparatus for providing security against unauthorized access to internal resources of a network device comprising:

a security association manager (SAM) configured to receive a digital signature;

wherein said SAM is configured to send a message including a portion of said digital signature;

wherein said message includes a request for an encryption decoder;

wherein said SAM is further configured to receive a response to said message; and

wherein said SAM is configured to send a digitally signed message requesting an access level for program code associated with said digital signature, in response to receiving said response message;

a policy server configured to receive said request for allowed operations associated with said authenticated signature;

said policy server including a comparison device configured to compare said authenticated signature with information stored on said policy server; and

said policy server being configured to send a response to said SAM indicating an access level corresponding to said authenticated signature.

13. (Currently Amended) Apparatus for providing security against unauthorized access to internal resources of a network device comprising:

means for receiving a digital signature including an encryption code;

means for requesting and receiving ~~aeeessing~~ a de-encryption code in electrical communication with said means for receiving;

means for de-encrypting and authenticating said digital signature;

means, responsive to said de-encrypting and authenticating of said digital signature, for obtaining an access level for a portion of program code associated with said digital signature; and

means, responsive to said access level, for determining allowed operations associated with said portion of program code responsive to processing of said portion of program code, wherein said allowed operations access said internal resources of said network device ~~digital signature~~.

14. (Original) Apparatus for providing security according to Claim 13 wherein said network device comprises a Java enabled device.

15. (Currently Amended) Apparatus for providing security according to Claim 13 wherein said portion of program code comprises a ~~further comprising~~ downloadable file ~~associated with said digital signature~~.

16. (Cancelled) Apparatus for providing security according to Claim 13 wherein said encryption code comprises a private key.

17. (Original) Apparatus for providing security according to Claim 13 wherein said de-encryption code comprises a public key certificate.

18. (Currently Amended) ~~Apparatus for providing security according to Claim 13 further comprising~~ Apparatus for providing security against unauthorized access to internal resources of a network device comprising:

means for receiving a digital signature including an encryption code;

means for accessing a de-encryption code in electrical communication with said means for receiving; and

means for determining allowed operations associated with said digital signature; and

means for receiving a downloadable filing including said digital signal and assigning an access level to a java thread.